Homeland Security News & Views

PENN STATE'S HOMELAND SECURITY NEWSLETTER

ISSUE 4, Spring 2015

Inside this issue:

Important Dates:

Spring 2015 commencement: Sunday, May 10

Summer session begins: May 18

Homeland Security Updater: August 3-7, 2015

Fall semester begins August 24

Welcome

Welcome to the fourth edition of News & Views!

The spring edition delivers a number of robust and interesting offerings and I want to thank everyone who contributed. It certainly makes my job easier! I especially want to thank our program alumni who contributed to this issue. We continue to seek input to the Newsletter from our graduates, as well as current students who are fully engaged in the homeland security enterprise. This is your opportunity to tell the rest of our *i*MPS-HLS community what's going on in the "world of work."

This issue has a wide variety of articles. In addition to the experiences of our alumni, this issue includes: articles on new course offerings; a cybersovereignty (a relatively new term) workshop at the Army War College; countering terrorist attacks with criminology; an exciting new opportunity to offer courses at the Marine Corps Recruiting Depot in San Diego, CA; and, of course our "In the Spotlight" segments.

We (the Program Office and faculty) frequently get asked, "How many students in your program?" or "How many graduates do you have now?" To address those "FAQs", if you will, we will include the small table below in each issue…fyi.

Thanks and I hope you enjoy this edition.

Tom Arminio

facebook.com/PSU.HLS

linkedin.com/groups/Penn-State-Intercollege-Master-Professional

iMPS-HLS Program Update

Graduates, December 2014: 47
Total graduates to date: 321
Anticipated graduates, May 2015: 48
Total graduates as of May 2015: 369
Current total student headcount (all Options): 1016

Message from the *i*MPS-HLS Program Chair

Dear Students, Alumni, and Friends of Penn State's Homeland Security Programs:

For our program, this spring semester 2015 has been a busy and successful one, with student enrollments reaching a new peak – we now have total of over 1,000 students in the intercollege Master of Professional Studies in Homeland Security (*i*MPS-HLS) program and to date graduated a cumulative total of 316 continuing and emerging leaders in homeland security.

A recent survey among graduates has shown that 60% of the respondents were "very satisfied" and 40% were "satisfied" with the overall education they received in our program. 91% said there were sufficient offerings to allow them to take classes suited to their career interests. 61% of respondents are employed in the public sector, which includes all levels of government, the military, emergency management, and law enforcement. 18% work in the private sector and 21% work in the IT sector (this could be public or private sector). Most respondents saw the cyber dimension and emergency management as the major challenges to homeland security.

The purpose of the program remains to:

Achieve excellence in higher education within the emerging and growing homeland security discipline to serve the future leaders of the homeland security enterprise, as well as those who seek to become leading future scholars in the field, giving full consideration to the requirements of employability and workforce transformation while teaching to the state of the art of the field.

At the same time, the program is reviewing the principles of homeland security education upon which it is based; the learning objectives; and the competencies that each and every student in this single-degree program has to achieve. The program will identify usable skills in a futuristic education framework, based on the most required knowledge and skill sets in the context of homeland security workforce transformation and input from the program Academic Advisory Council. In addition, Options and the Base Program define and review on a regular basis their specific educational principles and objectives.

The program has proven to be well aligned with the enduring core missions as well as with the risk-informed priorities of homeland security, as identified in the Department of Homeland Security's 2014 Quadrennial Homeland Security Review, the DHS Fiscal Plan 2014-18, and the new U.S. National Security Strategy of 2015, which concludes,

> "America's strategic fundamentals are strong but should not be taken for granted. We must be innovative and judicious in how we use our resources to build up our national power. Going forward, we will strengthen our foundation by growing our economy, modernizing our defense, upholding our values, enhancing the resilience of our homeland, and promoting talent and diversity in our national security workforce."

Our program is proud of making a contribution in an area where our talented students can flourish.

I would particularly like to draw your attention to our continuing education program, if you are an alumnus of our program and would like to return to your Alma Mater for a week this summer to receive an update on the latest trends in homeland security. Also, if you are otherwise interested in continuing education in homeland security, you are more than welcome to join this *Homeland Security Updater II short course* from August 3-7, 2015 (see p. 13). By completing additional lessons and assignments online, our current students may earn 3 500-level credits with this course.

I wish you a very nice spring time!

With best regards,

Alexander Siedschlag
Professor and Chair of Homeland Security

Updates from the Field:
Emerging Issues and Current Trends

Cybersecurity in the age of Terror and Foreign Adversary Aggression

Photo: Courtesy of Isiah Jones

by Isiah Jones

One could argue that cybersecurity is by far the most important homeland security, national security and public safety issue of our time. In the age of terror specifically, groups like ISIS, Al Shabaab, and AQAP have managed to use the internet to recruit and successfully spread their radical message of hate with little to no counter narrative of merit. Cybersecurity has rightfully been picked up and vocalized by the President as a top national and homeland security priority. With the increase usage of technology by nation states, rogue groups, and specifically terrorists with their growing focus on attacking the West, cybersecurity must be treated with the utmost importance.

Here is the problem: We still treat cybersecurity like it's just an IT problem or worse a compliance problem. Cybersecurity must be seen from, trained for, understood from, planned from, and executed from a broader perspective than IT and or compliance. Risk to the U.S. economy, infrastructure, and public safety warrant far more than the IT and/or compliance outlook on security issues. We have many IT savvy folks in the United States, as well as auditors and superb legal minds. However, we have a huge shortage of what I call hybrids; those people who can see across the various spectrums and domains of the issues of our time and tie cybersecurity into those issues ubitiquously. Those people are rare but greatly needed.

The other problem: There is a lack of true leadership for cybersecurity. Not merely a lack of leadership, but a lack of well-rounded cybersecurity professionals who are hybrids that also have or possess leadership skills, authority, and influence throughout the nation. Without more cybersecurity professionals obtaining such status and influence then we should expect many of the issues of our time to continually go unresolved in the manner in which they could or should be resolved.

Here is how we fix it: We need to emphasize, encourage and fund continuous learning. We also need to teach broad methodologies as the standard such as what most the International Information System Security Certification Consortium, Inc., (ISC)²® creates within its community of Certified Information Systems Security Professionals (CISSP). But bringing everyone both technical and non-technical together for one global and broad standard is only the beginning. Next, we have to continue deeper dives in various areas such as critical infrastructure control systems malware analysis, forensics, and penetration testing.

Furthermore, we must remove the culture of training just for the sake of maintaining the certifications and shift instead to a culture of continuous learning as a mode of survival and prosperity for the United States. Lastly, we must focus on enabling our people with the combination of higher education, certifications, continuous training, practice labs, and on-the-job experiences. Instead of picking between them, we need to encourage and accept the aggregate of them all. If we do these things we can begin to close the resource gap while also shifting the focus to becoming as agile as we need to be in these very uncertain times of terrorism, transnational organized crime, cyber criminals, and hackers.

Isiah Jones is a 2007 graduate of PSU with a BS in IST and a 2012 graduate of the *i*MPS-HLS Program in the Information Security and Forensics option. His certifications include: CompTIA Security+ce and ISC2 CISSP – Certified Information Systems Security Professional. He is currently a cybersecurity consultant for critical infrastructure industrial control systems (ICS)/Operational Technology (OT) related systems with Risk Mitigation Consulting, Inc (RMC). You can read more at: https://www.linkedin.com/pub/isiah-jones/17/449/7a3

Updates from the Field:
Emerging Issues and Current Trends

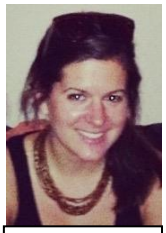

Photo: Courtesy of Caroline Walsh

Non-illness absenteeism and healthcare workers: Factors affecting willingness to work during a pandemic

by Caroline Walsh

Response preparedness and the well-being of my fellow first responders have always been topics of great research interest to me. In earning my Master's in Homeland Security from Penn State, I combined my undergraduate knowledge in Psychology, my graduate focus in Public Health Preparedness, and my active duty experience in the U.S. Coast Guard to produce relevant research related to a variety of homeland security topics. My research in homeland security included addressing the issue of interagency collaboration in port security operations to prevent agroterrorism and identifying narcoterrorist threats and trends in areas of Latin America and the Middle East. For my thesis, I branched out of the maritime environment to address hospital preparedness during pandemic situations. Hospital preparedness is a topic that arises when disaster strikes, most recently, SARS, Avian Influenza, and Ebola have brought attention to the issue of hospital readiness for pandemic-type situations. Hospitals have Emergency Action Plans for these conditions and conduct drills to prepare for containment, however, the question in the background that has not directly received enough attention remains, how many healthcare workers (HCWs) will be willing to show up to work during a pandemic?

The quest to identify who would be willing to work originated from the idea that during a pandemic, hospitals would be inundated not only with genuinely sick patients, but also with the "worried well." At a time when it is necessary to have all HCWs ready to respond, this type of mass casualty scenario could potentially create a situation in which the least amount of workers would be willing to come to work. For instance, in response to the Ebola outbreak and related events in the United States through October and November 2014, some nurses planned to conduct work stoppages, demanding improved safety precautions[1]. With HCWs at the front line of pandemic response, it is important to address HCW's safety concerns in regards to pandemic response to lessen HCW non-illness absenteeism during a pandemic. The study question became, what cross-cultural factors are associated with HCW non-illness absenteeism during a pandemic? Evidence was acquired though a systematic review of studies that examined HCW non-illness absenteeism during a pandemic. A total of 28 studies were included in the final review.

From the 28 reviewed studies, the most common factors found to be related to HCW's non-illness absenteeism were:

- general fear of illness (factor found in 15 [53.6%] of the articles);
- concerns for or obligations to family (n=14, 50%);
- lack of on the job communication or knowledge of pandemic and response information (n=13, 46.4%);
- concerns regarding personal protective equipment (n= 9, 32.1%); and
- concern in regards to workplace preparedness (n=5, 17.9%).

General fear and concerns for family were the most likely factors to contribute to HCWs' non-illness absenteeism during a pandemic. HCWs reported that they feared responding during a pandemic because of the risk that they would cause their family to become exposed to the agents and thus become ill. HCWs also reported that their family obligations, such as taking care of children or sick family members would be a barrier to reporting to work during a pandemic. There were results from various studies indicating that provision of safeguards to HCWs' family members would increase HCW's willingness to work during a pandemic. The findings from the studies indicate that nurses may be at higher risk to non-illness absenteeism. Of the 21 (75%) articles that examined multiple

[1] http://www.sfgate.com/bayarea/article/Kaiser-nurses-plan-two-day-strike-over-Ebola-5859514.php

categories of HCWs, almost one-third (n=6, 28.6%) included results that indicated that nurses might be at the highest risk for non-illness absenteeism during a pandemic.

It is necessary to identify and address the psychological aspects related to pandemic response that will affect HCWs' willingness to work. Regardless of HCWs' devotion to duty, there are additional factors that play a role in encouraging a full scale response. It is apparent from this systematic review that fear, lack of information, and concerns regarding protective equipment could be enough to cause some HCWs to remain at home and miss work during a pandemic. It is possible that incorporation of family plans concerning the safety of children and spouses, combined with further communication, training, and education for HCWs, will lead to a confident willingness to respond in a high risk environment.

Caroline Walsh is a Vulnerability Analyst with Strategic Operational Solutions working with the DHS Office of Cyber and Infrastructure Analysis. She recently received a direct Commission to the U.S. Coast Guard Reserve Officer program and was also accepted to George Mason University's graduate certificate program in Global Health and Security. She is a May 2013 graduate of the *i*MPS-HLS Program in the PHP Option.

Photo: Courtesy of Jason Sanford

The Right Background Makes a Difference

by Jason W. Sanford

What can I say? This kind of work is exciting and rewarding. Not one day is the same in emergency preparedness. At least in Georgia, it seems as though we are either responding to one event or planning for the next. As a state government official, I serve everyday knowing that the task is real, the stakes are high, and the cause could not be nobler. Since I started with the Georgia Department of Public Health as a Vulnerable Population Healthcare Coordinator in January 2014, the importance of understanding the principal homeland security and emergency management concepts and objectives has been quite evident. Penn State's intercollege Master of Professional Studies in Homeland Security (*i*MPS-HLS) Program helped prepare me for my current position in the Department's Office of Emergency Preparedness and Response.

As an *i*MPS-HLS student I selected the Base Program and I always appreciated the course offerings as well as the instructors who gave me a deeper understanding of policies, strategies, and critical thinking skills necessary to be successful. The Office of Emergency Preparedness and Response has a vast portfolio and I work with a plethora of health and emergency response professionals. The *i*MPS-HLS Program is unique in that it exposed me to various disciplines which has allowed me to understand terms and concepts and thrive no matter in which context I find myself.

For instance, in January 2014, Georgia experienced extreme winter weather and ice events which paralyzed the region and metropolitan Atlanta. Everything shut down. Businesses were closed and roads were blocked by tree limbs broken from the weight of the ice. Some long term care facilities (nursing homes) did not have power and at-risk dialysis patients did not have access to their critical medical treatment. The National Guard had to be deployed to transport patients to clinics and provide generators to those nursing homes without power. Furthermore, the regional infrastructure was not built to handle this type of severe weather. Since then, we continue to meet with our dialysis healthcare providers and have been working on building whole-of-community resilience and continuity of operation planning (COOP) among community stakeholders. The *i*MPS-HLS Program gave me an in depth understanding of the incident command structure and other key concepts that helped me overcome these and similar challenges and the skills necessary to coordinate a mitigation strategy. The *i*MPS-HLS Program also provided me with knowledge of risk management and multifaceted approaches to understanding roles and responsibilities of various stakeholders, which I find

important in building partnerships and healthcare emergency preparedness coalitions.

Georgia has seen terrorism (Centennial Olympic Park bombing in 1996), Ebola (first US Ebola patient treated successfully at the Centers for Disease Control and Prevention and Emory University), and extreme weather events like ice storms, wildfires, droughts, floods, tornados, and hurricanes (coastal evacuation planning). The *i*MPS-HLS Program has provided me with a richer understanding of terrorism and natural disasters which is something that I rely on often in preparing for, responding to, recovering from, and mitigating against the effects of disasters.

In April, I will be speaking at the National Preparedness Summit being hosted here in Atlanta and I consider it a privilege to be recognized as an alumnus of Penn State's *i*MPS-HLS Program.

Jason Sanford is a 2012 graduate of Penn State's *i*MPS-HLS Program. He previously earned a Master of Public Health Disaster Management from Benedictine University of Lisle, IL in 2010.

'Pathways' to Homeland Security

by Will Powell

When I first entered the *i*MPS-HLS Program at Penn State, my primary expectation was to learn factual information, as well as focus on theoretical approaches to new and existing problems in homeland security and homeland defense. From the onset of the very first lesson that pushed us to think of the boundaries of what "homeland security" actually means, my initial thoughts went to policy and factual know-how. What I did not expect was how directly many of the resounding themes and foundational elements of the *i*MPS-HLS Program would relate to an actual position working with the Department of Homeland Security.

As an *i*MPS-HLS student who was not actively working within the government or in a position or organization related to homeland security, I spent plenty of time combing through the USAJobs.gov website to find possible entry level positions or internships to give me the practical experience that the *i*MPS-HLS Program reinforced. The Pathways Program, initiated by President Obama, provided just that kind of opportunity. Open to current students and recent graduates, Pathways was intended to assist young men and women with getting their foot in the door to potential careers with the federal government. In my case, I applied for and was accepted for a Pathways position with the Federal Emergency Management Agency (FEMA), which is, of course, a component agency of the Department of Homeland Security.

From day one, I was able to see how many of the legal statutes, directives, and policies covered extensively in the *i*MPS-HLS Program were applied and provided a crucial foundation to FEMA and its mission. Whether it was the Robert T. Stafford Act, Homeland Security Presidential Directive 5 - Management of Domestic Incidents, or Presidential Policy Directive 8 – National Preparedness, the Pathways Internship allowed me to see how these major policy documents and statutes contributed and were intrinsic to day-to-day operations. In this respect, the Program came alive and I was able to use many of the skills emphasized in the program, whether it was critical thinking, writing specific action documents such as Bottom-Line-Up-Front (BLUF), and performing the other duties I was charged with as a Pathways intern.

Ultimately, I graduated from the *i*MPS-HLS Program and was later offered a full-time position with FEMA. The Pathways Program was an opportunity to turn the education I was receiving through the *i*MPS-HLS curriculum into action and moving knowledge into practice. Now, I work for FEMA Region III in External Affairs and I continuously refer back to many of the core documents and materials we reviewed in the *i*MPS-HLS Program to successfully execute my new role. I encourage everyone who wants to start in the federal government but is not of sure where to begin to consider the Pathways Program. It provided me with not only an opportunity to immerse myself in the field I was studying, but to also put into practice many of lessons learned and see how homeland security is carried out every day.

Updates from the Field: Emerging Issues and Current Trends

For information on the Pathways Program see: https://www.usajobs.gov/StudentsAndGrads

Will Powell is a 2014 graduate of the *i*MPS-HLS Program.

Penn State MOOC introduces geospatial intelligence to students around the world

by Hilary Appelman, happelman@psu.edu

January 14, 2015

UNIVERSITY PARK, Pa. — Geospatial intelligence was born of the defense industry, but Todd Bacastow said it can have broader applications in business and law enforcement as well.

Bacastow, the lead faculty member in Penn State's geospatial intelligence program, hopes Geospatial Intelligence and the Geospatial Revolution, a free online course that started Jan. 14, helps broaden the appeal of the discipline beyond the world of defense, both in and outside the United States. "This is a sort of swords-to-plowshares effort," Bacastow said. "Often in the United States geospatial intelligence is tied to U.S. intelligence agencies. I untie it."

The massive open online course, or MOOC, is offered through Coursera. More than 19,000 students enrolled — two thirds from outside the United States. Bacastow said he designed the course to provide a global perspective on GEOINT.

The five-week course explores the application of geospatial intelligence, or GEOINT, principles to business, emergency management and law enforcement as well as defense. A business might use GEOINT, for example, to decide where to locate a new inter-city air transport service, using residential and business demographics obtained from public (U.S. Census) and private sources. Participants learn how to use and apply GEOINT methods and also discuss questions of secrecy. The course culminates with a project in which students use real data to decide where to locate an Ebola treatment facility in Liberia.

The course follows Penn State's first geography MOOC, the wildly popular Maps and the Geospatial Revolution, which was offered again in March. Another course called Geodesign: Change Your World will be offered in July.

Penn State offers a graduate certificate in geospatial intelligence analytics and geospatial intelligence options in the MGIS and *i*MPS-HLS through its online World Campus.

Penn State's 5-week MOOC explored the application of geospatial intelligence, or GEOINT, principles to business, emergency management, and law enforcement as well as defense. Image: Penn State

The course was developed with the help of mapping software company ESRI, geospatial information provider DigitalGlobe, and the U.S. Geospatial Intelligence Foundation, which will staff a course discussion forum.

Penn State's new geospatial intelligence MOOC, led by Todd Bacastow, Ph.D., is designed to provide a global perspective on geospatial intelligence (GEOINT).

Image: Penn State

Dr. Todd Bacastow, the lead faculty member in Penn State's geospatial intelligence program, is teaching the MOOC: Geospatial Intelligence and the Geospatial Revolution.

Updates from the Field: Emerging Issues and Current Trends

Photo: Courtesy of Penn State Harrisburg

Explaining and Countering Terrorist Attacks with Criminology

by Jennifer Gibbs, Ph.D.

Terrorism is the intentional "use of illegal force and violence [by non-state perpetrators] to attain a political, economic, religious or social goal through fear, coercion or intimidation" (LaFree & Dugan, 2007, 184; National Consortium, 2014). Because terrorism is illegal violence that occurs outside International Humanitarian Law (that is, it targets noncombatants), it is crime and falls within the purview of criminology – the study of rule-making, rule-breaking and responses to rule-breaking (Sutherland & Cressey, 1978).

As a criminologist, part of my research explores factors associated with terrorism. Lately, my focus has been on terrorist attacks targeting the police. Police make attractive targets for some terrorists because they are representatives of the government's coercive authority, making them accessible symbolic targets. Some terrorist groups in the United States even have "hit lists" targeting police officers (Freilich & Chermak, 2009) because police are in a "brotherhood with the enemy government" (Miller, 2010). Also, as first responders to emergencies, police are tactical or strategic targets for terrorist groups. By overwhelming or incapacitating law enforcement, they become ineffective in resolving a terrorist attack, making the incident much bigger and more fatal.

Studying 82 countries around the world and using a variety of data, a few factors consistently emerge as important predictors of such attacks. First, in line with Pape's (2003, 2005) hypothesis, the presence of a foreign military (in any capacity) significantly increases the proportion of terrorist attacks targeting the police. Similarly, countries engaged in civil or inter-state conflict have a higher proportion of such attacks than countries at peace. Greater societal schism – that is, countries with minority groups that are very different from the dominant group in terms of language, customs, beliefs, and race – is associated with a higher proportion of terrorist attacks targeting the police, as is greater relative economic deprivation (measured by the Gini index). Finally, corrupt governments significantly increase the proportion of these terrorist attacks.

So, what should global policymakers do with this information? Foreign militaries can reduce their visible presence within a country, yet remain nearby through off-shore balancing (Pape, 2005). Governments should carefully consider state-sanctioned violence, as civil and interstate war are related to increased terrorist attacks. Societal schism and inequality can be reduced through giving representatives of minority and underprivileged groups "voice" – that is, allow everyone a seat at the table to participate in political decisions that affect their group (Dugan & Young, 2009). While some may consider this akin to negotiating with terrorists, ensuring representation to non-violent minority groups is a different animal. Finally, combatting corruption and increasing both police and government legitimacy can be accomplished through better training (see Bayley & Perito, 2010) and perhaps a focus on building trust between the police and the public so citizens are more inclined to share information with police to prevent possible attacks.

Additional research is needed to evaluate whether any of these policy suggestions effectively reduce terrorist attacks targeting the police and whether these explanations apply to other targets. Regardless, criminology has a lot to offer to the study of terrorism and counterterrorism.

Note: Dr. Gibbs gave a presentation on her research at the monthly Penn State Harrisburg (PSH) series "Academic Perspectives on Current Events." "Academic Perspectives" is intended to provide a faculty panel-audience discussion on timely issues. It is also directed at showcasing PSH faculty expertise. These sessions are free and open to the College community and the public.

Dr. Gibbs earned her Ph.D. in Criminology and Criminal Justice from the University of Maryland, College Park, where

she completed her dissertation focusing on the influence of police and state legitimacy on terrorist attacks targeting police in 82 countries. Dr. Gibbs joined the faculty at Penn State Harrisburg in 2013 as an Assistant Professor of Criminal Justice in the School of Public Affairs.

References:

Bayley, D. H., & Perito, R. M. (2010). *The police in war: Fighting insurgency, terrorism, and violent crime*. Lynne Reinner Publisher.

Dugan, L., & Young, J. (2009). Allow extremist participation in the policy-making process. In N. A. Frost, J. D. Freilich, & T. R. Clear (Eds.), *Contemporary issues in criminal justice policy: policy proposals from the American Society of Criminology conference* (pp. 159-168). Belmont, CA: Wadsworth.

Freilich, J. D., & Chermak, S. M. (2009). Preventing deadly encounters between law enforcement and American far-rightists. *Crime Prevention Studies, 25*, 141-172.

LaFree, G., & Dugan, L. (2007). Introducing the Global Terrorism Database. *Terrorism and Political Violence, 19*, 181-204.

Miller, C. D. (2010, April 8). Hutaree tapes: David Bryan Stone, Sr. rants against "new world order," say prosecutors. *CBS News*. Retrieved June 15, 2010 from http://www.cbsnews.com/8301-504083_162-20002051-504083.html

National Consortium for the Study of Terrorism and Responses to Terrorism. (2014, August). *Global Terrorism Database*. Retrieved July 25, 2014, from http://www.start.umd.edu/data/gtd/

Pape, R. A. (2003). The strategic logic of suicide terrorism. *The American Political Science Review, 97*(3), 343-361.

————. (2005). *Dying to win: the strategic logic of suicide terrorism*. New York: Random House Trade Paperbacks.

Sutherland, E. H., & Cressey, D. R. (1978). *Criminology* (10th ed.). Philadelphia: Lippincott.

Cyberthreat agency would focus defenses in United States

by Andrew Conte
Tuesday, Feb. 10, 2015, 8:42 p.m.

CARLISLE, PA — If President Obama's proposed new agency to coordinate federal cybersecurity efforts leads to increased information sharing among government agencies and private companies, that will improve defenses against hack attacks all around, experts gathered here this week said.

The new Cyber Threats Intelligence Center announced Tuesday by Lisa Monaco, assistant to the president for homeland security and counterterrorism, would coordinate the expertise the government has that now is spread across the U.S. Cyber Command, the FBI, the National Security Agency, the Department of Homeland Security and other agencies.

Similar competing bureaucracy issues impacted terrorism intelligence before the 9/11 attack, and White House cybersecurity coordinator Michael Daniel wants to resolve problems before attacks on American companies like Sony's movie subsidiary become even more serious. The cyber threats agency will be modeled after the National Counter Terrorism Center, which was established after 9/11 to coordinate terrorism intelligence.

"It's great to get some focus on cyber security. What we're hearing in industry and government is that it all needs to be improved, and these are great steps moving forward," Robert Clark, a cyber law fellow in the Army Cyber Institute at West Point told the Tribune-Review.

Clark is among more than three dozen cyber and legal experts from the military, government and private sector meeting this week at the U.S. Army War College in Carlisle to discuss cyber sovereignty. The Trib has been permitted to participate in the closed-door event.

Obama plans to host a cybersecurity summit at Stanford University on Friday, where he is expected to announce more details about the new cyber threats agency and government efforts to thwart hackers.

Updates from the Field:
Emerging Issues and Current Trends

Hackers are likely to exploit more sectors of the economy and to attempt more disruptive attacks, said Ronald Plesco Jr., chair and co-founder of the National Cyber Forensics & Training Alliance, based in Pittsburgh's Second Avenue technology corridor.

The president's initiatives are making everyone more aware of the need to defend against computer attacks, Plesco said.

“I'm encouraged that it's a top-of-mind issue for the administration and for the agencies — DHS, NSA and others,” Plesco told the Trib after giving a presentation at the workshop. “... It's putting it into the mainstream.”

Hackers do not care about the legal or policy obstacles that prevent companies and the government from sharing information more openly, he said. They are just using malware and approaches to exploit vulnerabilities in systems.

With a growing dependence on the Internet, agencies and corporations need to set a solid foundation for governance of networks, Plesco said.

“The approach has to be eyes wide open,” he said, “and to understand all of the competing interests, which they're doing.”

U.S. companies have been bombarded by a series of damaging cyber incidents in recent years — some from nation states, others from criminal groups. The Sony hack resulted in a variety of different analytical papers from various federal agencies, all concluding North Korea was responsible but with varying degrees of confidence.

Unlike the National Counter Terrorism Center, which gets most of its information from intelligence agencies, the new cyberagency may rely to a much larger extent on private companies, which are regularly seeing and gathering cyberintelligence as they are hit with attempts by hackers to break into their networks.

Gathering threat signatures, and profiling hacker groups, has become a key component of collecting cyberintelligence — a discipline practiced by government agencies and private firms.

U.S. intelligence officials have been warning about the dangers of cyberattacks for years, and the public is starting to pay close attention.

Fifty-seven percent of Americans in a new Associated Press-GfK poll conducted Jan. 29-Feb 2 think there is an extremely or somewhat high risk of a foreign country or terrorist group making a major cyberattack on computer systems inside of the United States. That is more than the 50 percent who say the risk of a terrorist attack is somewhat or extremely high.

On the other hand, fewer Americans say the risks posed by computer hackers are important to them personally (57 percent) than say the same of terrorism (71 percent).

Just over half of Americans, or 51 percent approve of the way Obama is handling threats posed by computer hackers, the survey found.

Tom Arminio, professor of homeland security at Penn State University in Harrisburg, said “there's a lot more that people can do” to protect themselves — “everybody who uses a computer or cell phone.”

“My fear is complacency,” he said. “That we're getting so accustomed to hearing about daily cyber attacks that it's just the course of doing business, and it shouldn't be.”

The Associated Press contributed to this report. Andrew Conte is a staff writer for Trib Total Media. He can be reached at 412-320-7835 or andrewconte@tribweb.com.
http://www.cyberrattlingtrib.com/

http://triblive.com/usworld/nation/7751746-74/cyber-agencies-government#axzz3RectWXI1

Retrieved February 13, 2015
Used with permission

In the News

HLS 803 - Homeland Security: Social and Ethical Issues - Course Redesign

by Joe Balay, Ph.D.

Beginning Summer Semester 2015, the *i*MPS-HLS Program will be rolling out a new version of its core course, *HLS 803: Homeland Security: Social and Ethical Issues*. The course is sponsored by the College of the Liberal Arts, and is intended to offer students a broad introduction to political and moral theory and its critical application to security issues today. The plan for the redesign grew out of last year's Program Retreat, and responds to both student feedback and program goals to better integrate the course's ethical-political emphasis (e.g. Aristotle, Mill, Kant, John Rawls, Naomi Zack) with applied topics in the homeland security field (e.g. ebola, immigration, drones).

The redesign will preserve the core of the previous course structure while supplementing these materials with a variety of media (e.g. Ted Talks, Case Studies, Discussion Forums) to practice informed ethical decision-making in the face of topical homeland security situations. At the heart of the redesign is an exciting new Case Study Database. The database was collaboratively created by the program faculty, representing each of the five program options, and focusing on current ethical debates in the homeland security field. These concise, 1-page case studies will be incorporated into the course alongside more traditional theoretical texts to help situate weekly discussions (e.g. on human rights in the context of mandatory vaccination debates). The Case Study Database will also be made accessible to the other iMPS-HLS program courses to encourage inter-program continuity, and to facilitate the examination of these issues in a host of specialized contexts.

The capstone of the new course will be the revised Group Final Project. For this project, students are divided into 5-person teams and tasked with producing an in-depth exploration of a contemporary homeland security ethics debate. In addition to producing a research paper on the topic, they will also generate their own 1-page case study. The best case studies will be considered for inclusion in the Case Study Database. In this way, students are provided with an opportunity to contribute to the future growth of the *i*MPS-HLS program, while gaining valuable experience producing an industry standard resource text.

Joe Balay received his Doctor of Philosophy from Penn State in 2014. He is currently a Lecturer in the Department of Philosophy.

New Course to be Offered in Homeland Defense and Defense Support of Civil Authorities

by Tom Arminio

This course, HLS-832, "The Military's Domestic Imperative: Homeland Defense (HD) and Defense Support of Civil Authorities (DSCA)," will explain the military's homeland defense mission and domestic support of civil authorities during disasters, and the distinctions between the two. Any prospective homeland security practitioner and member of the homeland security enterprise should understand the basics of the Department of Defense's (DOD) and the National Guard's respective roles, missions, and functions in protecting the homeland and providing civil support. This elective course will be offered beginning fall semester 2015.

There is nothing obvious or intuitive about the employment of the United States military within the United States. The decision to use the military in civil support functions is always made with careful consideration. Over time, the American public has come to value and expect the military's response to domestic disaster emergencies. Likewise, DOD has developed protocols and doctrine to accommodate those expectations within the necessary constraints of its mission and its place in society. This points to a long-standing tradition that has given a role to the military that safely secures its status as *one* element of national power, *not the one and only* controlling element. This balance and the foundational concept of civilian control of the military must be understood by all homeland security practitioners and the future leaders of the homeland security enterprise.

The distinction between homeland security and homeland defense is significant. Too often the

uninitiated will assume that homeland defense is a subset of homeland security or worse, use the terms interchangeably or synonymously. They are, in fact, distinct but related functions. The difference is very important to understand in as much as responsibility for homeland defense lies with DOD and responsibility for homeland security lies with DHS.

Title 10 active duty forces, the separate Services' reserve components, and the states' and territories' National Guard may all be called upon to respond to a request for assistance during a domestic emergency. DOD's philosophy here is that the military's support in domestic operations is a "total force" effort. This can be seen as tying directly into the established tiered response concept during a disaster emergency; and the military's response may well begin…and most often will end…with the National Guard, and grow as required with additional resources from the Service Reserves and active component (Tussing, 2014).

Other core concepts support the "total force" aspect of DOD's support to disasters. First, during a DSCA mission, the military will always be in a support role. Second, before military assets are requested and introduced in support of a domestic requirement, the existing civil capabilities and resources should be applied (to the fullest extent practicable). Third, DOD is ever mindful of ensuring against the military becoming unnecessarily involved in a long-term commitment in an affected state or community. DSCA missions should be limited in duration and scope (Tussing, 2014).

Defense support in the wake of a catastrophic natural disaster is by no means the end of potential DSCA missions. Any number of other situations or crises could require DOD capabilities, e.g., major terrorist attack, border security, or pandemic flu. Title 10 DOD assets will, of course, always be prepared to serve at the direction of the President. Similarly, State National Guard assets will always be prepared to serve at the direction of the Governor.

Penn State University has a longstanding and rather extensive relationship with DOD. For example, the Applied Research Lab provides solutions to problems in national security and is a U.S. Navy Affiliated Research Center, designated by DOD, and maintains a long-term strategic relationship with the Naval Sea Systems Command and Office of Naval Research (www.arl.psu.edu). Additionally, certain faculty members of the *i*MPS-HLS Program's Geospatial Intelligence Option have a long-standing relationship with the National Geospatial Intelligence Agency (NGA). Penn State Harrisburg and the Office of Military and Security Programs have partnered for the last four years in the Intelligence Community Center of Academic Excellence (IC CAE) grant. The executive agent for the IC CAE grant is the Defense Intelligence Agency (DIA). Ensuring *i*MPS-HLS students understand how DOD can assist in the preparedness, protection, prevention, response, recovery, and mitigation construct will have long-lasting, positive influence in any organization in which alumni serve.

Tom Arminio is a Lecturer in the *i*MPS-HLS Base Program.

New Course Offered on Cyber-Geography in Geospatial Intelligence

by Michael L. Thomas, Ph.D.

Cyber-Geography in Geospatial Intelligence (GEOG 479) examines the landscape of cyberspace, the geopolitics of cyberwar, techniques that might be employed in such a conflict and how they are related to censorship on the Internet, ideas on regulation and network architecture, the politics of censorship and hacking, and the politics of grassroots activism enabled by cyber Internet Communication Technologies (ICT). Students will examine simple information systems, the emerging landscape defined by the "geographies of the Internet," and the impacts as they concern the intersection of ICTs and intelligence. The course will be centered on fundamental geospatial intelligence concepts with emphasis on technology, information theory, and geopolitics.

In the News

Many of the failures in the intelligence community can be traced back to a severe misunderstanding of what GeoCyber is and what it is not. Without a thorough understanding of the effects of Geography on Cyber, efforts are doomed to be ineffective. For example, while much ink has been spilled on the topic of ISIS activity on social media, very basic questions remain unaddressed, including such fundamental issues as how many social media users support groups like ISIS, who they are, and how many of those supporters take part in its highly organized online activities.

Three years after the Arab Spring, repressive governments have taken the lessons learned from the dictators' downfalls and seem to be using the same technologies to counter nascent opposition movements inside the country before they can get organized. Retired U.S. Army General Stanley McChrystal once observed that "it takes a network to fight a network." Before the fight can even begin, understanding exactly what a network really is must take place. The connections between networks, cyber, and geography are real and are what make GEOG 479 a "must take."

Along with teaching in the Geospatial Intelligence Option, Dr. (LtCol, USAF) Thomas is currently assigned to the Naval Space and Warfare Systems Center as a C4ISR Systems Engineer in the Communications and Networks Division. Dr. Thomas received his Ph.D. in Information Systems from Argosy University, Sarasota, FL

Continuing Education Residential Short Course—P ADM 597A.201: Homeland Security Update II

Penn State Harrisburg, Middletown, PA
August 3-7, 2015

Based on an all-hazards approach, this intensive residential short course provides a cross-disciplinary overview of current trends and research in homeland security and its evolving mission space – including comparisons to other countries, as well as in the overarching perspective of civil security. The course has a modular structure with lectures and micro-seminars given by Penn State faculty and guest lecturers, including subject matter experts from the U.S. Homeland Security Enterprise and the international community.

The course also comprises an excursion to the Pennsylvania Criminal Intelligence Center (Fusion Center) in Harrisburg, with expert briefings, interactive syndicate group work, and networking receptions.

Course topics include:

- Homeland security today and challenges ahead;
- Intelligence for homeland security;
- Emerging threat analysis;
- Critical infrastructure vulnerability and risk assessment (with an on-campus case study);
- Process control for cybersecurity;
- Public health preparedness: Trends and future implications;
- Centers of Disease Control and Prevention;
- Research for homeland security in Europe and transatlantic collaboration;
- Good practices in crime prevention and security management in global supply chains; and
- Comparative homeland security .

Graduate credits option:

By completing some lessons and assignments online before and after the residential short course week, students may earn 3 500-level credits.

For more information and course topic updates, please visit:

http://harrisburg.psu.edu/courses/homeland-security-update-research-and-trends

---

In the News

Sony Pictures hack redefines rules of online warfare

by Andrew Conte
Thursday, Feb. 12, 2015, 11:30 p.m.

When hackers broke into computer systems at Sony Pictures Entertainment in a failed attempt to stop the release of “The Interview” late last year, the cyberattack changed the way top American military policymakers look at online warfare, experts say.

Electronic skirmishes that had played out quietly among computer technicians at a hacked company and a federal agency contacted for advice instead went all the way to the Oval Office, as President Obama blamed the Sony incident on a nation-state attack by North Korea.

“In the Sony case, it moved from the commander's inbox to the commander-in-chief's inbox, and that's the first time that's happened,” Navy Capt. Joel Doolin told cybersecurity experts gathered here at the U.S. Army War College. “That's why we're talking about it. It was extraordinary.”

In an interview with the Tribune-Review, Robert Clark, a cyber law fellow in the Army Cyber Institute at West Point, agreed: “The Sony hack showed how we work through a sliding scale. It moved from a criminal act to a terrorist threat attributed to a nation-state, and now the Department of Defense and the president have a role.”

As Obama made plans to host a cybersecurity summit Friday with industry leaders at Stanford University, more than three dozen military officers, Defense industry engineers and academics met here separately Tuesday through Thursday to discuss recommendations for military policies of cyber-warfare. The Trib was granted permission to attend the closed-door meetings.

The group's recommendations include requiring utilities and other critical infrastructure companies to share information about computer threats, and freeing up more government intelligence in return.

Policymakers suggested minimum cybersecurity requirements for Defense Department contractors, stronger capabilities for identifying hackers, and better deterrents against foreign online attacks.

They called for eliminating laws against companies that take offensive steps to thwart hackers. And they see a need for clearer lines when a criminal act becomes a cyberattack that triggers a military response.

When Obama called the Sony incident a cyberattack and blamed North Korea, that changed that vector for discussing online war policy, said Bill Waddell, director of the War College's Mission Command Cyber Division, who moderated the workshop.

Attacks among nation-states are easy to understand when they happen on the ground, at sea or in the air — but Internet intrusions can be hard to detect and harder still to defend, participants said. Private-sector companies control 80 percent of the Internet domain, questions of civil liberties must be considered, and enemies with limited resources can exact major damage.

“The fact that we have become so dependent on the use of (the Internet) creates that type of vulnerability,” Waddell said. “The Defense Department looks at its responsibility to protect, to fight the nation's wars, to keep enemies at bay, to provide deterrents — and is trying to figure out, ‘How does that fit in cyberspace?' ”

The discussion raises difficult questions. Workshop participants debated even how to define cyberspace and online warfare.

When members of one smaller group discussed top international cyber players besides the United States, debate arose about whether to identify specific countries before a majority decided to name Russia, China, North Korea and Iran.

Some ideas discussed at the War College are taking effect. When Obama appears at Stanford, he is expected to detail plans for a Cyber Threats Intelligence Center, focused on sharing government intelligence among agencies and with private companies.

“You have a spectrum of bad behaviors that can happen in cyberspace,” said Capt. Doolin, the primary legal adviser to the deputy chief of Naval Operations for Information Dominance. “What the Sony case proves is:

In the News

'Hey, we the United States have a spectrum of responses we can take.' "

The Associated Press contributed to this report. Andrew Conte is a staff writer for Trib Total Media. He can be reached at 412-320-7835 or andrewconte@tribweb.com.
http://www.cyberrattlingtrib.com/
http://triblive.com/usworld/nation/7751746-74/cyber-agencies-government#axzz3RectWXI1

Retrieved February 13, 2015
Used with permission

Penn State to offer courses to military community at San Diego Marine base—

Agreement with Marine Corps Recruit Depot will expand access to a Penn State education through World Campus

March 18, 2015

UNIVERSITY PARK, Pa. — Penn State will begin offering select courses this fall at the Marine Corps Recruit Depot in San Diego with the goal of giving military personnel more access to a college degree.

The courses, from defense- or business-related academic programs, will be taught in a dedicated Penn State classroom at the Marine Corps Recruit Depot via Penn State World Campus, the University's online campus. The site will be the University's first classroom on a military base.

The academic operations will be managed by Penn State World Campus through a five-year agreement with the Marine Corps, and military personnel who take classes on-site will be registered as World Campus students. The agreement calls for on-site face-to-face instruction, which is designed to orient military personnel into an education setting for them to finish their degrees online through World Campus.

"We are excited to expand access to higher education to the San Diego military community," Penn State President Eric Barron said. "The University has a long history of educating members of our armed forces, and we are committed to providing them with a high-quality academic experience and the opportunity to become part of the Penn State community."

The San Diego area has one of the largest concentrations of military installations in the country, which include Naval Base San Diego, Naval Amphibious Base Coronado and Marine Corps Air Station Miramar. Within a 15-mile radius of the Marine Corps Recruit Depot, there are more than 55,000 military personnel, according to the Department of Defense's 2012 Demographics Report, which has the most recent data available.

Penn State will have its first dedicated teaching site on a military base this fall, when select courses through Penn State World Campus will be offered at the Marine Corps Recruit Depot in San Diego. The courses will be available to military personnel in the San Diego area, and the courses are part of defense- and business-related academic programs.

Image: Marine Corps photo by Lance Cpl. Jericho W. Crutcher

Select courses from the following degree programs will be taught through the Marine Corps Recruit Depot classroom:

- Master of professional studies in homeland security
- Master of professional studies in supply chain management
- Master of professional studies in human resources and employment relations
- Bachelor of science in labor and employment relations

Once students have completed the courses offered at the depot, they can continue their academic program online through World Campus to finish their degrees.

"Penn State World Campus is providing another option for a high-quality college education to the military community in San Diego," said Craig Weidemann, vice president for outreach and vice provost for online education at Penn State. "The classroom environment is an important element to help our military students

transition into an online educational setting. Finishing their degree online through Penn State World Campus will be a good fit for them because they can study when it's convenient from wherever they are in the world."

World Campus will begin renovating the classroom space in spring 2015 for classes to begin in August, the start of the University's 2015 fall semester. In addition to the classroom space at the depot, World Campus will have office space for an on-site admissions counselor and an outreach director.

Currently, 17 percent of World Campus's 10,805 students are military-affiliated students.

For more information about resources for online military students, visit the World Campus's website.

State's new emergency management director reflects on his Penn State experience

Jennifer Miller
March 18, 2015

PEMA Director Richard D. Flinn Jr. addresses the media during a press conference with Gov. Tom Wolf at PEMA headquarters Jan. 26, 2015.
Image: Commonwealth Media Services

Decades before Richard Flinn, Jr. became head of emergency management operations for the Commonwealth of Pennsylvania, he was working as an emergency medical technician (EMT) at Penn State, teaching first aid courses to students and faculty members across the state, and earning a bachelor of science degree in health planning and administration.

Today, Flinn, who Gov. Tom Wolf recently appointed as director of the Pennsylvania Emergency Management Agency (PEMA), oversees statewide response to disasters and initiatives to prevent and reduce the effects of disasters.

A combination of his time serving as a firefighter, EMT and paramedic; more than 35 years of military experience; and academics, including his time at Penn State, prepared Flinn for his new role.

At Penn State, Flinn said he gained many critical skills he still utilizes today, such as public speaking, interpreting statistical analyses, and other skills specific to emergency management. "What I learned at Penn State, from a planning perspective, is the idea of really understanding how you look at a problem," Flinn said. "First defining a problem, working your way through it, coming up with various courses of action and then developing an implementation plan."

To Penn State and back

In 1972, Flinn enrolled at Penn State Beaver with an interest in journalism and experience as a sports writer. A year later, during the Vietnam War, Flinn began his military career by enlisting in the U.S. Army as an active duty combat medic and medical clinical specialist from 1973-76.

Next, Flinn enrolled at University Park to complete his bachelor's degree. With extensive emergency response and medical experience on his resume, Flinn changed his area of study to health planning and administration. While studying, he served as an EMT at University Park. Instead of tailgating before football games, he sat on the hood of an ambulance inside Beaver Stadium ready to assist with medical emergencies.

"Years later, I took my son to a game and experienced tailgating for the first time," Flinn said. "It was a tremendous experience."

While studying, David Lindstrom, former director of emergency preparedness in the College of

Medicine at Penn State, became Flinn's mentor. During summer breaks, the pair traveled to Penn State campuses teaching instructors a continuing education course in classroom emergency care. Flinn also instructed first aid courses to students at University Park. "If it wasn't for Lindstrom and Penn State, I probably wouldn't be sitting here today," Flinn said.

Turning education into action

Lindstrom, a member of Pennsylvania Emergency Health Services Council, helped Flinn become involved with one of the council's committees at Penn State. The council is a nonprofit mandated by state law to serve as the state advisory council to the Secretary of Health regarding emergency health services.

After graduating in 1979, Flinn became a safety engineer for U.S. steelworkers in Pittsburgh. Four months later, the council offered Flinn a position in Harrisburg where he helped develop a comprehensive emergency medical system for Pennsylvania. Flinn worked for the council for 24 years and ultimately became executive director.

Wolf appointed Flinn as director of PEMA in January. He is also a member of the governor's cabinet. "My goal is to make us one of the best emergency management agencies in the country," Flinn said. Flinn said he plans to enhance the agency by strengthening relationships with fellow cabinet members and emergency managers at the county level. He also plans to enhance relationships with a broader community.

"Disasters are not just government centric," Flinn said. "They involve entire communities. It's not a PEMA disaster; it's a commonwealth disaster. We will work closely with county emergency managers, but also other government agencies, the private sector and academia."

Specifically, Flinn noted the impact academia has on emergency management, from research to community outreach. "There are over 25 colleges and universities throughout the country that offer degrees in emergency management. Research from lessons learned after events, to studying human behavior, to examining how we are organized in an emergency operations centers and many other topics are and will be invaluable to improving how government, the public, the private sector and the voluntary organizations prepare for, respond to, mitigate and recover from disasters," Flinn said.

As director, Flinn also plans to build a relationship with state climatologist Paul Knight, who is based at University Park, to examine how climate change and weather events are changing "so that we can better understand and be prepared to respond to new and different weather events in the commonwealth."

He also noted the student-organized Penn State-Michigan State Blood Challenge for the American Red Cross, now in its 21st year. "That's a great program that exists and is a way to get young people involved in emergency management," Flinn said.

Most recently, Flinn served as the deputy director of the Operations Division at the Federal Emergency Management Agency (FEMA) headquarters in Washington, D.C., where he assisted the director in overseeing the National Response Coordination Center, the National Watch Center, the FEMA Operations Center at Mount Weather, the National Incident Management Teams, and the National Urban Search and Rescue Program.

From September 2005 until October 2010 Flinn served as deputy director for PEMA. Prior to joining PEMA, Flinn worked for the Pennsylvania's Governor's Office of Administration as the special assistant for Continuity of Government.

Flinn has more than 35 years of military experience and retired in December 2013 from the Pennsylvania Army National Guard as the

commander for the Pennsylvania Medical Command with the rank of colonel. He has more than 40 years of experience in emergency services, serving as a firefighter, EMT and paramedic. He served as a volunteer fire chief and a township emergency management coordinator for more than 10 years.

Flinn has a master's degree in governmental administration from the University of Pennsylvania. He is also a graduate of the U.S. Army Command and General Staff School, and is a certified emergency manager from the International Association of Emergency Managers.

Jennifer Miller can be reached at:
Jlm966@psu.edu
814-865-8465
Reprinted with permission.

New Homeland Security Books

This is information is provided to help you expand your professional library.

- Marion, Nancy E., Kelley A. Cronin, and Willard M. Oliver. *Homeland Security: Policy and Politics.* Durham, NC: Carolina Academic Press, 2015.

  A comprehensive analysis of controversial issues in the still emerging field of homeland security, focused on law enforcement and emergency management. Topics covered include the history and future of FEMA; DHS funding; fusion centers; intelligence-led policing; evolution of the terrorist threat; role of citizen volunteers in disaster response; cybersecurity; immigration policy; transportation network safety; etc.

- Martin, Gus. *Understanding Homeland Security.* Los Angeles, CA et al.: Sage, 2015.

  A comprehensive discussion that addresses areas such as emergency management, terrorism, criminal justice administration, intelligence, armed conflict, and social environments, as well as critical thinking. Theories, agency missions, laws, and regulations governing the U.S. homeland security enterprise are reviewed to help the reader understand the dynamic and evolving nature of the homeland security mission space.

- Oliver, Willard M., Nancy E. Marion, and Joshua B. Hill. *Introduction to Homeland Security: Policy, Organization, and Administration.* Burlington, MA: Jones & Bartlett, 2015.

  Geared to entry-level personnel and supported by an extensive online resource space, this book provides an accessible overview of homeland security concepts, definitions, policies, and organizations addressing foundational issues, as well as political, legal, and technological responses to the contemporary challenges.

- Sylves, Richard. *Disaster Policy and Politics: Emergency Management and Homeland Security.* 2nd ed. Washington, D.C. et al.: CQ Press, 2015.

  This text covers emergency management as a part of the homeland security mission space, using an all-hazards approach and public management as well as historical, legal, and science and engineering perspectives, as well as mini-case studies from the U.S. and some other countries. The practical focus is on the role of decision makers at the federal, state, and local levels; scientists; engineers; civil and military personnel; officials; and first responders.

- Vermeulen, Gert, and Wendy De Bondt. *Justice, Home Affairs and Security: European and International Institutional and Policy Development.* Antwerpen: Maklu, 2015.

  This text covers the historical, institutional, and topical development of the EU policy in the

areas of justice, home affairs and security, embedded in a broader international context including the Council of Europe, NATO, OSCE, G8/G7, OECD, and the UN.

Spotlight

Student in the Spotlight

The Power of Partnership

by Sean Cooley

*i*MPS-HLS GEOINT option student Sean Cooley at the 2015 ESRI Federal GIS Conference in Washington, DC, in February. Photo: Courtesy Sean Cooley

What is the result when more than 3000 geographers, map heads, intelligence analysts, geo geeks, and academics hangout for a few days? *Partnership!*

The ESRI Federal GIS Conference consisted of two days packed full of discussion panels, breakout sessions, a robust exhibition hall, and a lineup of distinguished speakers including ESRI founder Jack Dangermont and two-term Maryland Governor Martin O'Mally. The conference aimed at targeting all facets of government including those that deal with the environment and resource management such as the National Oceanic and Atmospheric Administration (NOAA) and the Environmental Protection Agency (EPA) to those that focus on protecting America's freedoms such as members of the Intelligence Community and the Department of Defense. This melting pot of agencies resulted in over 150 presentations with a wide range of topics including: Sharing Tradecraft with ModelBuilder and Geoprossessing Services; ArcGIS for the Military; and Thinking Spatially with GIS. Regardless of the diverse topics, one theme rang constant: Partnership.

The theme of partnership was perhaps best illustrated by Director Robert Cardillo in his keynote address. Cardillo, the new director of the National Geospatial Intelligence Agency (NGA) stressed three major points during his presentation. First, that we as geospatial practitioners make certain we use our tools, techniques, and data to shape decisions. Second, he challenged the geospatial community, particularly the NGA, to lead the Intelligence Community in transparency. He explained that the NGA is already spearheading that initiative by providing informational features such as an NGA Twitter and by providing over 25% of NGA's data to be publicly accessed via the NGA website for anyone to read and interact with. Finally, Cardillo stressed the need for the NGA and the geospatial community to form partnerships.

Several examples of partnerships that Cardillo offered during his address included the NGA's Ebola Map which helps monitor and control the Ebola epidemic in West Africa. He explained, that through partnerships with the Liberian Government, the NGA was able to work with that nation's mapping specialists to provide them with crucial knowledge and training used to manage the virus's spread. Another partnership that Cardillo highlighted was that of the NGA's relationship with Penn State University in creating the first ever Massive Open Online Course (MOOC) focusing on Geospatial Intelligence and the Geospatial Revolution. Director Cardillo went on to recognize Penn State's own Dr. Todd Bacastow; praising him and the University for their efforts to spread GEOINT education to a global audience. Cardillo noted that with over 12,000 course attendants in 183 countries the Penn State MOOC is inspiring a previously untapped number of people. Moreover, he proclaimed that he himself is taking the course having already worked through the first four lessons. He hopes that the MOOC will inspire a new generation of GEOINT professionals.

Cardillo closed by saying that it is the individual that makes everything possible and that when he is briefing the president, the information, maps, and intelligence used were provided by individuals who helped make it all possible. So whether it is two nations allying to fight disease, the Director of the NGA addressing the President, or a room full of entry level analysts working on their next mapping assignment, the thing that makes it all possible is…well, I think you get the picture.

Sean Cooley is a student in the Geospatial Intelligence Option of Penn State's *i*MPS-HLS Program. He has an anticipated graduation date of 2016.

Spotlight

Faculty in the Spotlight

William J. Ryan
Protective Security Advisor - Philadelphia, PA
U.S. Department of Homeland Security

by Tom Arminio

Photo: Courtesy of Bill Ryan

William J. Ryan joined the Department of Homeland Security as a Protective Security Advisor (PSA) in February 2005. As a PSA, Mr. Ryan contributes to the development of the national risk picture by assisting with the identification, assessment, and monitoring of critical infrastructure. He also acts as a physical and technical security advisor to federal, state, and local law enforcement agencies, as well as the private sector.

Prior to assuming his PSA duties, Mr. Ryan served as an intelligence officer in the Central Intelligence Agency's (CIA) National Clandestine Service (formerly the Directorate of Operations) from 1998 to 2005. Mr. Ryan's assignments included tours in both the overseas and domestic fields, as well as at CIA headquarters.

Before joining the CIA, Mr. Ryan was an International Programs Specialist with the Department of the Navy from 1991 to 1998. During his tenure with the Navy, Mr. Ryan negotiated the transfer of U.S. military equipment to foreign government allies to assist in securing U.S. interests overseas, as well as the interests of the respective countries.

Mr. Ryan holds a Master of Business Administration degree from Drexel University in Philadelphia and a Bachelor of Science degree from the University of Delaware. He is also a Lecturer of Homeland Security in Penn State's *i*MPS-HLS Program.

This is Mr. Ryan's first semester teaching in the Base Program. As a Homeland Security practitioner and "end user" of *i*MPS-HLS Program graduates, he has been a terrific addition to the faculty.

To date, his teaching has been both personally and professionally rewarding. "The experience has been fantastic, as the students with whom I interact on a regular basis have some innovative ideas and informed opinions when it comes to Homeland Security. I have attempted to guide students to get to a point where the can relate those ideas and opinions to concrete examples—showing them that often times their thoughts are not just theory, but are applicable to the real world of the homeland security enterprise. In my opinion, the discussions that bring in real world events to exemplify a thought process, or to bear out an idea, are extremely useful and interesting."

"Those that have real world experience have put forth points of view that have supported, and added to, what I have imparted to the class; and in some cases have given me a different way of looking at issues. Additionally, those with little experience in the field have provided valuable insight into the suppositions made about Homeland Security. All in all, it has been a very rewarding experience."

Upcoming Events

Spring 2015 commencement: Sunday, May 10

Summer session begins: May 18

Homeland Security Updater II (residential short course)
Date: August 3-7, 2015
Location: Penn State Harrisburg
URL: http://harrisburg.psu.edu/courses/homeland-security-update-research-and-trends

Contact Information

Tom Arminio
(717) 948-6649 | tja12@psu.edu
777 W. Harrisburg Pike | Middletown, PA 17057